VIAVI Solutions

How a NetOps/SecOps Alliance Can Outmaneuver the Enemy

Winning the Security Battle eBook

NetOps and SecOps are Allies

The time for Network Operations and Security Operations slugging it out in the war room is long past. Network service assurance and security issues are inextricably linked.

So, it makes sense that the NetOps and SecOps teams are as well.

To beat the hackers, it's time to join forces, tear down the silos, and sign the peace treaty.

The organization is under siege on every front.

An insurgent hacker only has to get lucky once.

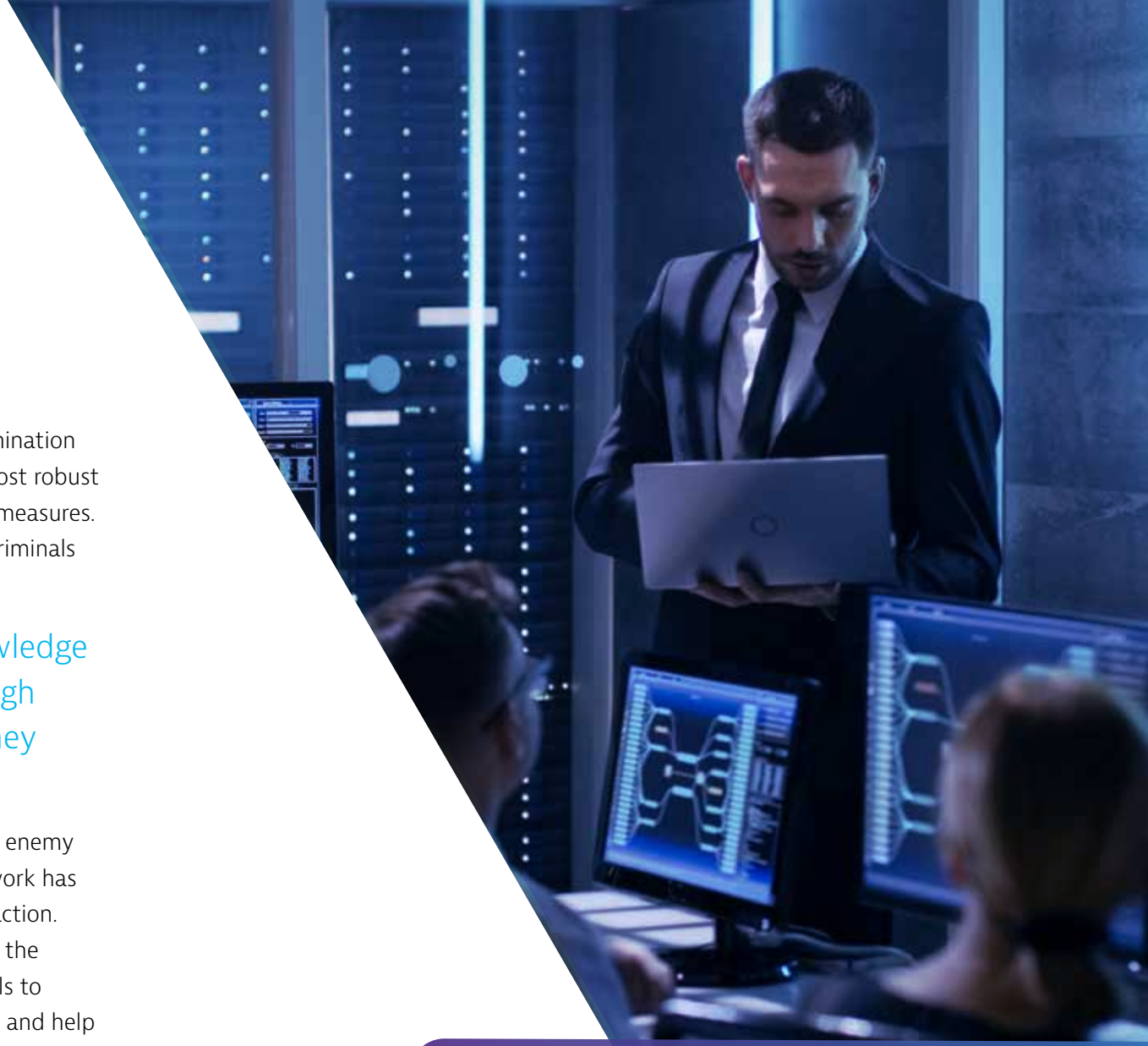
The organization has to be lucky 24/7 to protect its employees, customers, investors, and reputation.

©2019 VIAVI Solutions, Inc

The increasing sophistication and determination of hackers spells disaster for even the most robust defence-in-depth preventative security measures. Threat vectors are increasing and cybercriminals are leveraging new hacking tools.

Most businesses now acknowledge that it's no longer good enough having plans in place for *if* they are breached.

Threat hunting to actively search for the enemy within, on the assumption that the network has been compromised already, is gaining traction. Likewise, organizations are waking up to the power of detection and remediation tools to identify an attack, contain the offenders and help the clean-up *when* they are breached.



©2019 VIAVI Solutions, Inc

Cyber Security by Numbers

Network teams are spending **more than 25% of the working week** resolving security issues

State of the Network Survey 2019

Security breaches have increased by 67% in the last 5 years with the annual cost of cybercrime increasing 72% in the same period. Banking, utilities, insurance, automotive and software organizations experience the highest annual costs associated with cybercrime

Accenture 2019 Cost of Cybercrime study

Email and malware threats are the fastest growing

State of the Network Survey 2019

The popularity of **using wire data for security incidents** has grown significantly in just two short years.

State of the Network Survey 2019, 2017

©2019 VIAVI Solutions, Inc

The 3 Security Phases

Until recently, the IT and budget focus has been on Prevention, some on Detection, and in a far distance third — Remediation. Organizations are beginning to realize that the focus must shift towards solutions that can offer the augmented and improved detection that comes from having granular data, with advanced traffic profiling and faster remediation for when a hacker inevitably does breach the defences.

$10.8 Billion
on Prevention
& Detection

$200 Million
on Remediation

Source: Gartner, Inc.

1. **Prevention** Hacker gets lucky once. Organization must be lucky enough to stop them 100% of the time.
2. **Detection** Know what's connected to the network, and what's communicating along with setting baselines, thresholds, and profiling traffic to trigger real-time alerts for abnormal activity. Enable threat hunting and root cause troubleshooting on complete traffic data.
3. **Remediation** Forensic analysis of who, what, when, where using every single transaction, or conversation, all the time, anywhere on the network.

©2019 VIAVI Solutions, Inc

Assessing the Threat Vector

Networks today face threats that are farther reaching and ubiquitous than they were even as recently as two years ago. When every bad guy in the world is less than 200ms away, anything and everything that is connected to the network from a wired, wireless or even a cellular perspective is a possible source for attack. Attack paths that exploit the weakest link, the human layer, are on the rise. And the hackers aren't just looking to steal data, but to change it or destroy it and sometimes just to disrupt and disable businesses. The different types of events and situations that network security teams face today seem insurmountable at times. It is therefore critical to understand what is connected and communicating on your network at any given moment.

> Attackers from around the globe are attacking these companies and, if compromised, can cause significant issues to the company's productivity, their compliance, and their reputation. Once the malware is already inside, we need to know how many users it has impacted, where exactly it has penetrated and in which directions, and what was it trying to do.

Sumit Dhoopar, Cyber security architect at a Fortune 100 company

©2019 VIAVI Solutions, Inc

Align Divided Forces

According to research undertaken by IDG*, having siloed Network and Cybersecurity teams is a recipe for disaster. Repercussions of this organizational dysfunction include:

- Slow response to security events
- Finger-pointing and loss of productivity
- Increases in security breaches and data loss
- Service downtime for customers and internal staff
- Inability to determine root cause of security events

The rallying cry needed to ensure NetOps and SecOps teams are pulling together is **visibility**. Shared visibility means teams see the same things and are working from the same data.

This visibility engenders confidence that comes from having a shared view of exactly what is happening on the network and agreeing upon the best actions to take based on that shared view.

This confidence, in turn, builds trust that problems can be understood, acted on and fixed faster and more efficiently than ever before without overlap, duplication or gaps.

*Source: *A House Divided: The Cost of Dysfunction Between Network and Cybersecurity Teams*, IDG, 2018

©2019 VIAVI Solutions, Inc

Although often separate, NetOps and SecOps teams share the common goal of maintaining secure, high-performance network infrastructures. Infrastructure and operations leaders can leverage shared data and tools to optimize budgets, avoid duplication of effort and improve the end-user's experience.

Align NetOps and SecOps Tool Objectives With Shared Use Cases by Gartner analysts Sanjit Ganguli and Lawrence Orans, July 24, 2018

©2019 VIAVI Solutions, Inc

5 Simple Steps to Forensic Truth

1. Find one single set of tools to power the network/security coalition. You all get to see the same data, analyze and act on it. It avoids the confusion, speculation and finger pointing.
2. Every piece of data matters. Don't prune it or throw any of it away. You never know what you'll need to get to the root of the problem quickly and reconstruct the breach later to ensure that nothing was missed.
3. Your network infrastructure has so much it could tell you, if only you would interrogate it. Every device on your network has information about north-south or east-west network traffic – captured via SNMP, flow data and/or packets. Uncover what they know. Gaps in your intelligence make for guesswork, wasted time, assumptions and bad decisions, so start asking!
4. False positives are your enemy. Don't get side-tracked by the decoys and distractions, and inadvertently head straight for the ambush. Baselining and advanced traffic profiling are the intel you need to keep you on the right route.
5. Use guided insight to quickly pinpoint the bad guy in real-time. Follow the path signposted by intelligent, automated workflow tools. They will indicate deviations from baselines and normal traffic profiles to reveal the culprit, assess the scope, impact and collateral damage, and help ensure the holes are plugged after the attack is repelled.

©2019 VIAVI Solutions, Inc

Answer three questions to begin your mission

Do you know what is (really) connected to your network?

Do you know what is communicating on the network? (and who is communicating back?)

Which tools do you have to answer these two questions?

©2019 VIAVI Solutions, Inc

Fortunately, innovations in technology, combined with advanced analytics, machine learning and rule-based detection are making it easier for enterprises to get ahead of security and service delivery issues.

VIAVI expands the scope of traditional flow by stitching it together with other seemingly disparate data records to create *enriched* flow records. The structured insights from enriched flow enable network security threat hunting and security management to become less ad-hoc and 'lucky' and be more automated, focused and continuous.

Combine data sources and consolidate tools to make it easier than ever for NetOps and SecOps to get the visibility they need to identify unauthorized devices and rogue activities and succeed in the war against the hackers.

©2019 VIAVI Solutions, Inc

Win the Security Battle

Stay one step ahead of user-impacting issues Minimize potentially disruptive outages by baselining normal network activity, alerting on anomalies, and profiling acceptable device behavior.

Consolidate tools across teams One unedited pool of data looked at from different angles is better than siloed or pruned information.

Find and fix issues faster Reduce business and reputational impact. Time IS money.

Support business growth Manage and optimize evolving, growing networks without introducing increased security risks.

©2019 VIAVI Solutions, Inc

VIAVI Solutions provides network performance and security tools that help customers to manage network infrastructure, and troubleshoot issues across physical, virtual, and cloud environments. VIAVI Observer Platform brings together NetOps and SecOps teams enabling them to use the same network data and tools. Intelligent insights and unparalleled network visibility enable IT departments to deliver optimal service levels while avoiding duplication of effort and protecting the organization against escalating security threats.

Our leading solutions, deep technical mastery and worldwide channel community of VIAVI Velocity Solution Partners, make VIAVI a trusted advisor to top enterprises worldwide.

viavisolutions.com/network-security-intelligence

© 2019 VIAVI Solutions Inc.
Product specifications and descriptions in this document are subject to change without notice. Network-security-intelligence-bk-ec-nse-ae | 30190923 900 1019

Contact Us

+1 844 GO VIAVI
(+1 844 468 4284)

To reach the VIAVI office nearest you, visit viavisolutions.com/contact

VIAVI